WHAT IS CLAIMED:

1. (Currently amended) A computer implemented method for evaluating a security risk of an application, said method comprising the steps of:

~~determining whether unauthorized access or loss of said data would cause substantial damage;~~

~~determining whether said application is vulnerable to attack by a third party;~~

determining whether the application is shared by different customers;

determining whether a third party can have unauthorized administrative authority to data maintained by said application;

determining whether a third party can have unauthorized read and/or write access to data maintained by said application;

~~determining mitigation controls for the security risk of said application; and~~

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

combining said numerical values or weights to evaluate said security risk.

Claim 2 (Canceled).

3. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said application is subject to industry controls for security; and

assigning a numerical value or weight to the determination whether said application is subject to industry controls for security, and using the numerical value or weight for the determination whether said application is subject to industry controls for security in evaluating said security risk.

Claims 4-6 (Canceled).

7. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether ~~said application is vulnerable to allow~~ a third party can have unauthorized read and write access to said data; and

assigning a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data, and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

8. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

assigning a numerical value or weight ~~corresponding to a significance of said security risk~~ to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs and using the numerical value or weight to the determination whether the vulnerability in said application can be exploited by a program or person which has not been authenticated to said application or a system in which said application runs in evaluating said security risk.

9. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said data maintained by ~~or accessed~~ by said application is confidential; and wherein

the numerical value or weight assigned to the determination whether a third party can have unauthorized write access to said data is based in part on whether said data is confidential.

10. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a customer has direct use of said application; and

assigning a numerical value or weight to the determination whether a customer has direct use of said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

Claim 11 (Canceled).

12. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is ~~wherein said mitigation controls comprise~~ an intrusion detection system and vulnerability scanning for said application; and

assigning a numerical value or weight to the determination whether there is an intrusion detection system and vulnerability scanning for said application, and using the numerical value or weight for the determination whether there is an intrusion detection system and vulnerability scanning for said application in evaluating said security risk.

Claims 13 and 14 (Canceled).

15. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is ~~wherein said mitigation controls comprise~~ a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

assigning a numerical value or weight to the determination whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems, and using the numerical value or weight for said requirement for authentication in evaluating said security risk.

Claims 16-18 (Canceled).

19. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

20. (Currently amended) A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

Claims 21-24 (Canceled).

Please enter new claims 25-32, as follows:

25. (New) A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable media;

first program instructions to determine whether the application is shared by different customers;

second program instructions to determine whether a third party can have unauthorized administrative authority to data maintained by said application;

third program instructions to determine whether a third party can have unauthorized read and/or write access to data maintained by said application;

fourth program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

fifth program instructions to combine said numerical values or weights to evaluate said security risk; and wherein

said first, second, third, fourth and fifth program instructions are recorded on said media.

26. (New) A computer program product as set forth in claim 25 wherein:

said third program instructions determine whether a third party can have unauthorized read and write access to said data;

said fourth program instructions assign a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data; and

said fifth program instructions also use the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

27. (New) A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

seventh program instructions to assign a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and wherein

said fifth program instructions also use the numerical value or weight to the determination whether the vulnerability in said application can be exploited by a program or person which has not been authenticated to said application or a system in which said application runs to evaluate said security risk; and

said sixth and seventh program instructions are recorded on said media in functional form.

28. (New) A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether a customer has direct use of said application; and

seventh program instructions to assign a numerical value or weight to the determination whether a customer has direct use of said application; and wherein

said fifth program instructions also use the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk; and

said sixth and seventh program instructions are recorded on said media.

29. (New) A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

fifth program instructions to assign a numerical value or weight to the determination whether there is said requirement for authentication; and wherein

said fifth program instructions also use the numerical value or weight for said requirement for authentication in evaluating said security risk; and

said sixth and seventh program instructions are recorded on said media.

30. (New) A computer program product as set forth in claim 25 further comprising:

sixth program instructions to compare the evaluation of said security risk to a cost savings provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said sixth program instructions are recorded on said media.

31. (New) A computer program product as set forth in claim 25 further comprising:

sixth program instructions to compare the evaluation of said security risk to a revenue provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said sixth program instructions are recorded on said media.

32. (New) A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable media;

first program instructions to determine whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs;

second program instructions to determine whether a third party can have unauthorized administrative authority to data maintained by said application;

third program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

fourth program instructions to combine said numerical values or weights to evaluate said security risk; and wherein

said first, second, third and fourth program instructions are recorded on said media.

33. (New) A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether a third party can have unauthorized read and/or write access to data maintained by said application; and

sixth program instructions to assign a numerical value or weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application; and wherein

said fourth program instructions also use the numerical value or weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application to evaluate said security risk; and

said fifth and sixth program instructions are recorded on said media in functional form.

34. (New) A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether a customer has direct use of said application; and

sixth program instructions to assign a numerical value or weight to the determination whether a customer has direct use of said application; and wherein

said fourth program instructions also use the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk; and

said fifth and sixth program instructions are recorded on said media.

35. (New) A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

sixth program instructions to assign a numerical value or weight to the determination whether there is said requirement for authentication of said application or said system; and wherein

said fourth program instructions also use the numerical value or weight for said requirement for authentication of said application or said system in evaluating said security risk; and

said fifth and sixth program instructions are recorded on said media.

36. (New) A computer program product as set forth in claim 32 further comprising:

fifth program instructions to compare the evaluation of said security risk to a cost savings provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said fifth program instructions are recorded on said media.

37. (New) A computer program product as set forth in claim 32 further comprising:

fifth program instructions to compare the evaluation of said security risk to a revenue provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said fifth program instructions are recorded on said media.